DOI: https://doi.org/10.53486/9789975155663.26
CZU: 004.056.5:005.334

THE ROLE OF RPO AND RTO IN DISASTER RECOVERY PLANNING

ROLUL RTO ȘI RPO ÎN PLANIFICAREA RECUPERĂRII ÎN CAZ DE DEZASTRU

Aureliu ZGUREANU[51]**, Assoc. Prof., PhD.**

Abstract:*As multiple research and surveys published in recent years show, disaster recovery is becoming an increasingly important factor in business continuity. Renowned British information provider IHS Markit states that organizations experience an average of 5 downtime events per month which is equivalent to 27 hours. This turns into significant losses or even leads to business closure. Careful disaster recovery planning is required to reduce losses, and two of the most important attributes used to measure the efficiency of the data protection and recovery process are the recovery time objective (RTO) and the recovery point objective (RPO). Based on the analysis of some recognized technical disaster recovery solutions, their related documentation and some publications of important specialists in the field, this article emphasizes the role of RTO and RPO in disaster recovery planning. As a result of the research, the place of RTO and RPO in information disaster recovery was highlighted, as well as the key elements in the calculation process of these two strategic recovery objectives.*
Key words*: RTO, RPO, Backup, Disaster recovery, Business continuity.*

Rezumat: *După cum arată multiplele cercetări și sondaje publicate pe parcursul ultimilor ani, recuperarea în caz de dezastru devine un factor tot mai important în continuitatea afacerii. Renumitul furnizor Britanic de informații IHS Markit afirmă că organizațiile în mediu experimentează 5 situații de nefuncționare pe lună ceea ce echivalează cu 27 de ore și se transformă în pierderi esențiale sau chiar duc la închiderea afacerii. Pentru reduce pierderile este necesar de o planificare minuțioasă a recuperării în caz de dezastru, iar două dintre cele mai importante atribute utilizate pentru măsurarea eficienței procesului de protecție și recuperare a datelor le reprezintă obiectivul timpului de recuperare (RTO) și obiectivul punctului de recuperare (RPO). În acest articol se face o analiza a soluțiilor tehnice de recuperare recunoscute, a documentației aferente acestora și a publicațiilor specialiștilor importanți din domeniu pentru a evidenția rolul RTO și RPO în planificarea recuperării în caz de dezastru. În rezultatul cercetărilor a fost evidențiat locul RTO și RPO în recuperarea informației, precum și trasate elementele cheie în procesul de calculare-estimare a acestor două obiective strategice de recuperare.*
Cuvinte cheie*: RTO, RPO, Recuperarea în caz de dezastru, Copie de rezervă, Continuitatea afacerii.*

JEL CLASSIFICATION: H12, M15

1. Introducere

Cel mai cunoscut investitor din zilele noastre, Warren Buffet[52], a spus o frază faimoasă: "*It takes 20 years to build a reputation and five minutes to ruin it*". Această frază se potrivește de minune cu o companie prosperă, recunoscută, însă care nu a acordat suficientă atenție planificării continuității afacerii, mai concret implementării unei soluții fiabile de backup și recuperare în caz de dezastru IT. Potrivit datelor furnizate de platforma Zerto, o corporație cu venituri anuale de 100 de milioane de dolari ar pierde în jur de 275.000 de dolari într-o perioadă de nefuncționare de 24 de ore (Zerto, 2020). Compania ar pierde doar în jur de 45.000 de dolari având implementat un program de replicare a instantaneelor de 4 ore și aproximativ 7600 de dolari utilizând replicarea continuă de „aproape-de-zero" ore. În practică, această sumă ar putea fi mai mică sau mai mare în funcție de ora zilei și de activitatea aplicației.

Este foarte important ca managementul superior al companiei să conștientizeze că situațiile de nefuncționare pot interveni în orice moment și că nimeni nu poate fi sigur că așa

[51] E-mail: Zgureanu.aureliu@ase.md, Academy of Economic Studies of Moldova.
[52] *Warren Edward Veirdo Buffett* (n. 30 august 1930, Omaha, Nebraska) este un investitor, om de afaceri și filantrop american. Este recunoscut ca fiind al 3-lea în lista celor mai bogați oameni din lume în anul 2006, pe al treilea loc în lista anului 2007 și primul pe lista anului 2009.

situații nu se vor întâmpla în compania lor. Starea de nefuncționare a întreprinderii cauzată de imposibilitatea din diverse motive de a accesa datele se numește dezastru, iar limitarea pierderilor în astfel de cazuri este parte a strategiei de continuitate a afacerii și implementată fără urme de neglijare.

În IT, un dezastru poate fi orice problemă neașteptată care duce la o încetinire, întrerupere sau o eroare într-un sistem cheie sau o rețea. Aceste probleme pot fi cauzate de dezastre naturale (adică incendii, cutremure, uragan, etc.), erori tehnologice, acte rău intenționate, diverse tipuri de incompatibilități sau chiar de simple erori umane. Probabilitatea ca un astfel de dezastru să aibă loc poate crește odată cu dezvoltarea organizației și a infrastructurii sale IT, a concurenței neloiale și a multor altor factori. Totodată, cea mai bună apărare orientată spre evitarea urmărilor dezastruoase ce pot apărea în astfel de situații constă în planificarea continuității afacerii și a recuperării datelor în caz de dezastru, folosind cele mai bune practici, soluții și strategii care ghidează organizațiile în prevenirea și/sau gestionarea mai bună a evenimentelor perturbatoare imprevizibile.

Ținând cont de ultimele date statistice, o organizație nu poate să-și permită riscul confruntării cu un dezastru IT fără a fi pregătită de astfel de scenarii, deoarece urmările perturbărilor datelor organizației, și implicit a reputației sale, o poate costa foarte mult, până chiar și la pierderea afacerii. Institutul Ponemon și IBM Security în raportul Cost of a Data Breach Report pentru anul 2020 a constatat că costul mediu al unei încălcări de date la nivel global este de 3,86 milioane de dolari (3,90 în 2019 și 3,86 în 2018) (IBM, 2020). Același raport pentru anul 2018 arată că 65 la sută dintre clienții cărora le-au fost compromise datele au spus că și-au pierdut încrederea într-o organizație, iar unul din trei a ales să-și întrerupă relația cu organizația afectată. În acest context recuperarea datelor capătă o conotație specială și devine una dintre elementele de bază ale managementului continuității unei afaceri.

2. Recuperarea în caz de dezastru IT

Standardul ISO/IEC 27031:2013: Tehnologia informației - Tehnici de securitate - *Linii directoare pentru disponibilitatea tehnologiilor de informare și comunicare pentru continuitatea afacerilor* specifică recuperarea dezastrelor IT ca capacitatea elementelor TIC ale unei organizații de a-și susține funcțiile critice de afaceri la un nivel acceptabil într-o perioadă de timp prestabilită după o întrerupere. În același document este definit și Planul de continuitate a afacerii (BCP -Business Continuity Plan) și Planul de recuperare în caz de dezastru TIC (ICT DRP – Disaster Recovery Plan) (SM, 2013).

Planul de continuitate a afacerii reprezintă un set de proceduri documentate care ghidează organizațiile să răspundă, să recupereze, să reia și să restabilească la un nivel predefinit de funcționare în urma întreruperii. În mod normal, aceasta acoperă resursele, serviciile și activitățile necesare pentru a asigura continuitatea funcțiilor critice ale afacerii.

Planul de recuperare în caz de dezastru TIC este un plan clar definit și documentat care recuperează capacitățile TIC atunci când apare o perturbare (uneori acesta se mai numește plan de continuitate TIC). Astfel, recuperarea resurselor IT în caz de dezastru este un set standard de politici și proceduri pe care o afacere sau o organizație le pune în aplicare și le urmează pentru a se proteja pe sine și personalul său în fața unui dezastru. Planurile de recuperare în caz de dezastru pot ajuta compania să asigure securitatea angajaților, a hardware-ului și software-ului, restaurarea sistemelor și a elementelor conexe continuității afacerii. DRP-urile pot include măsuri preventive, măsuri corective și măsuri detective pentru a preveni cât mai mult posibil dezastrele care ar putea afecta întreprinderile, reducând în același timp, într-un mod cât mai fiabil posibil, impactul unui dezastru (Zgureanu, 2020).

Măsurile preventive sunt acele măsuri care diminuează riscul și previn apariția unui dezastru IT, iar exemplele de aceste măsuri includ backup-ul datelor în cloud, efectuarea de audituri de securitate de rutină, etc. Măsurile detective ajută la descoperirea potențialelor

amenințări, de exemplu, actualizarea software-ului antivirus, instalarea software-ului de monitorizare server/rețea etc. Măsurile corective conțin pașii necesari pentru restabilirea rapidă a sistemelor IT lovite de dezastru. Toate aceste măsuri sunt importante în realizarea procesului de recuperare IT și de aceea trebuie tratate cu responsabilitate maximă.

Recuperarea în caz de dezastru - cunoscută și sub numele de recuperare în caz de dezastru IT este una dintre discipline legate de continuitatea afacerii, iar secțiunea A.17 din anexa A la standardul ISO/IEC 27001 are ca obiectiv pentru o organizație încorporarea continuității securității informațiilor în sistemele sale de gestionare a continuității activității. Pentru a susține acest lucru, această secțiune oferă controale legate de procedurile de continuitate a afacerii, planuri de recuperare și redundanțe (SM, 2017).

Cu toate acestea, la fel ca toate standardele sistemului de management, ISO 27001 descrie doar ceea ce trebuie realizat, însă nu și cum. Însă familia ISO/IEC 27000 are standarde suplimentare care vizează domenii specifice, iar unul dintre ele este ISO/IEC 27031, care acoperă disponibilitatea tehnologiei informației și comunicațiilor pentru continuitatea afacerii (sau IRBC - ICT Readiness for Business Continuity) și ne ghidează cu privire la ce trebuie să luăm în considerare atunci când dezvoltăm continuitatea afacerii pentru IT - de obicei, aceasta se numește „recuperare în caz de dezastru" (SM, 2013). Implementarea ISO/IEC 27031 devine tot mai actuală odată ce tot mai multe activități ale companiilor moderne au devenit dependente de tehnologiile informației și comunicațiilor, iar erorile și defecțiunile IT devin din ce în ce mai critice.

În acest context, standardul ISO/IEC 27031 abordează modul de utilizare a ciclului PDCA (Plan-Do-Check-Act) pentru a pune în aplicare un proces sistematic de prevenire, prezicere și gestionare a incidentelor de perturbare a serviciilor TIC sau a celor care au potențialul de a perturba aceste servicii (SM, 2013). Procedând astfel, acest standard ajută la susținerea atât a managementului continuității afacerii, cât și a managementului securității informațiilor. Prin natura sa, ISO/IEC 27031 este un standard perfect pentru realizarea controlului A.17.2.1 din ISO/IEC 27001 (disponibilitatea mijloacelor de prelucrare a informației) (SM, 2017).

Este adevărat că termenul de recuperare în caz de dezastru nu este un termen oficial ISO și, în consecință, sensul său nu este universal acceptat. Cu toate acestea, majoritatea profesioniștilor IT identifică acest termen cu capacitatea de a recupera infrastructura IT în caz de perturbare. Prin urmare, ISO 27031 este cel mai potrivit dintre standardele ISO anume în acest scop.

Este necesar aici de precizat unele diferențe esențiale între ISO 27031 și ISO 22301 - *Securitate şi stabilitate. Sisteme de management al continuităţii activităţii. Cerinţe* (ISO, 2012), care se referă direct la continuitatea afacerii. În primul rând, ISO 22301 acoperă continuitatea afacerii în ansamblu, considerând orice tip de incident ca o sursă potențială de perturbare (de exemplu, boală pandemică, criză economică, dezastru natural etc.) și utilizând planuri, politici și proceduri pentru a preveni, reacționa, și recupera după perturbările cauzate de acestea. Aceste planuri, politici și proceduri pot fi clasificate în două tipuri principale: cele pentru continuarea operațiunilor, dacă afacerea este afectată de un eveniment de perturbare și cele pentru recuperarea infrastructurii IT, în cazul în care sunt perturbate tehnologiile IT.

Prin urmare, ne putem gândi la ISO 27031 ca la un instrument pentru implementarea părții tehnice a ISO 22301, oferind îndrumări detaliate cu privire la modul de a face față continuității elementelor TIC pentru a ne asigura că procesele organizației vor oferi clienților rezultatele așteptate.

ISO 27031 recomandă șase categorii principale care necesită a fi luate în considerare la planificarea continuității afacerii cu referință la elementele care implică TIC și care pot răspunde la întrebările principale care apar în procesul de asigurare a continuității (SM, 2013):

1. *Abilități și cunoștințe*: strategiile de recuperare includ luarea în considerare a abilităților tehnice specializate și a cunoștințelor necesare pentru a opera serviciile IT până la, în timpul și după o perturbare; strategiile care includ considerări privind abilitățile și

cunoștințele se concentrează pe asigurarea faptului că niciun individ nu deține abilități sau cunoștințe specializate care ar fi necesare pentru a opera sistemele IT ale organizației.
Aici trebuie luate în considerare:

- informațiile care sunt necesare pentru a rula serviciile IT critice;
- persoanele care dețin aceste informații;
- modul în care pot fi încorporate aceste informații în cunoștințele organizaționale și puse la dispoziție cu ușurință;
- modul în care organizația face disponibile aceste informații în caz de dezastru.

2. *Echipamente*: strategiile de recuperare includ reducerea riscului asociat cu operarea sistemelor TIC bazate pe un singur echipament; strategiile care includ considerări privind echipamentele asigură utilizarea sistemelor IT chiar dacă echipamentul primar devine inoperabil.
   Pentru aceasta este necesar de avut în vedere:
   - condițiile care ar trebui să le respecte dispozitivele și infrastructura pentru a minimiza riscurile de perturbare sau timpul de recuperare;
   - locul unde ar trebui amplasate astfel de facilități.
3. *Tehnologia*: strategiile de recuperare includ luarea în considerare a cerințelor tehnice necesare pentru a îndeplini cerințele de recuperare ale organizației, în special Obiectivul Timpului de Recuperare (RTO) și Obiectivul Punctului de Recuperare (RPO); strategiile mai includ considerări tehnologice care implică asigurarea faptului că hardware-ul și software-ul și datele pot fi recuperate în timpul solicitat de organizație.
   Aceste considerări ar trebui să includă:
   - tehnologiile cele mai importante pentru afacere - sisteme de asistență, cum ar fi alimentarea, răcirea, personalul, asistența furnizorului și conectivitatea WAN;
   - cerințele de recuperare, de exemplu, RTO, RPO, dependența de alte tehnologii, etc.
4. *Date*: strategiile de recuperare includ luarea în considerare a modului de protejare a datelor solicitate de organizație.
   Strategiile privind datele includ:
   - securitatea, validitatea și disponibilitatea datelor solicitate de utilizatorii finali;
   - datele necesare pentru a restabili activitățile comerciale și în ce perioadă de timp (de reținut că RTO și RPO pentru serviciile IT sunt diferite de RPO și RTO pentru date);
   - controalele de securitate (de exemplu, controlul accesului) care trebuie să existe în permanență pentru a securiza datele.
5. *Procese*: strategiile de recuperare includ luarea în considerare a modului de susținere a proceselor necesare pentru a monitoriza, opera și recupera sistemele IT pentru a satisface cerințele afacerii; strategiile care iau în considerare procesele identifică procesele IT necesare înainte, în timpul și după o întrerupere a sistemelor IT și anume:
   - procesele pe care le avem la dispoziție pentru a face față unui incident sau dezastru;
   - modul în care procesele necesare pentru a crea elemente din categoriile 1-4 funcționează împreună pentru a furniza serviciile comerciale necesare (de exemplu, comunicații, aplicații, acces utilizator etc.).
6. *Furnizori*: strategiile de recuperare includ luarea în considerare a modului de informare și implicare a furnizorilor care sunt necesari pentru recuperarea și operarea sistemelor TIC.
   Aceste strategii definesc:
   - furnizorii implicați în operarea și recuperarea sistemelor TIC înainte, în timpul și după ce a avut loc o întrerupere;

- consumabilele (de exemplu, copii de software și piese de schimb hardware) esențiale pentru continuitatea IT, modul în care se pot asigura furnizorii companiei că pot susține cerințele de continuitate a afacerii acestei companii.

3. Locul RTO și RPO în recuperarea în caz de dezastru

Observăm că RTO - obiectivul timpului de recuperare, precum și RPO - obiectivul punctului de recuperare, reprezintă niște elemente-cheie, care trebuie luate în considerare la planificarea continuității afacerii. Pe lângă aceste două atribute ale evaluării eficacității soluțiilor de protecție și recuperare a datelor mai putem enumera fereastra de backup, dar și cheltuielile generale repartizate pentru recuperare. Acești parametri descriu intervalul dintre două operații de realizare a copiilor de rezervă, durata procedurii de restaurare efectuată în caz de eroare, defect sau dezastru, precum și timpul alocat pentru a face copiile de rezervă.

Fiecare dintre aceste trei atribute reprezintă, de asemenea, o măsură a timpului de nefuncționare: timpul necesar pentru a reconstitui datele noi, care nu au fost încă salvate, timpul care trebuie petrecut pentru operațiunea de recuperare și timpul în care datele nu sunt disponibile în timpul procesului de backup. În funcție de locul în care se află sistemul și datele protejate în organizație, durata de nefuncționare cauzată de operațiunile de protecție sau recuperare va afecta într-un fel sau altul indicii financiari.

Fereastra de backup este intervalul complet (inclusiv timpul necesar pentru pornire și oprire) necesar pentru a face backup unui anumit sistem sau set de date. Dacă întreprinderea poate scurta timpul necesar pentru crearea copiilor de rezervă și pentru a reduce sau chiar elimina fereastra de backup, apare posibilitatea de a recupera eventualele profituri pierdute (Veeam, 2021).

În trecut, administratorii de backup făceau multe operații manual, ceea ce influența direct mărimea ferestrei. În prezent însă, politicile inteligente, automatizarea sistemului, tehnologiile de descoperire automată, utilizarea stocării pe disc și replicarea la un centru de recuperare în caz de dezastru pot ajuta la minimizarea eforturilor și la reducerea costurilor. Aceste caracteristici și abordări ajută la eliminarea celei mai mari părți ale muncii manuale și a timpului cheltuit pentru operațiuni de protecție a datelor. Cu toate acestea, multe companii continuă să urmeze vechea metodă, abandonând utilizarea copiilor de rezervă sau externalizarea acestor funcții către furnizori independenți de servicii, punând astfel în pericol funcționalitatea normală a afacerii.

Pentru a îmbunătăți disponibilitatea datelor, a reduce riscul și costurile, toate organizațiile, mari și mici, ar trebui să aplice tehnologii moderne de protecție a datelor. Cu astfel de soluții, spre exemplu cu cea oferită de Hitachi (Hitachi, 2020), fereastra de rezervă poate fi minimizată sau chiar eliminată. Aceste rezultate sunt obținute prin tehnologii de protecție continuă a datelor (CDP- Continuous Data Protection) integrate la nivel de bloc și compatibile cu aplicațiile pentru snapshot-urui, care sunt făcute utilizând hardware dedicat. În rezultat se elimină necesitatea scanării sistemului de fișiere pentru a găsi modificări incrementale și reduce timpul necesar copierii datelor la câteva secunde.

Obiectivul timpului de recuperare (RTO – Recovery Time Objective) este *perioada de timp* necesară pentru a recupera operațiunile normale de afaceri după o întrerupere. Atunci când încercăm să stabilim care este RTO, va trebui să luăm în considerare cât timp de nefuncționare este dispusă compania să piardă și care este impactul pe care îl va avea acest timp asupra afacerii. RTO poate varia foarte mult de la un tip de afaceri la altul. De exemplu, dacă o bibliotecă publică își pierde sistemul de cataloage, ea poate continua să funcționeze manual timp de câteva zile, în timp ce sistemele sunt restaurate. Dar dacă de exemplu un retailer online își pierde sistemul de inventar sau datele despre încasarea plaților online, chiar și pentru 10 minute de întrerupere, pierderea asociată a veniturilor și disconfortul creat clienților ar fi inacceptabile.

ISO 22300, care definește vocabularul pentru ISO 22301, oferă o definiție pentru obiectivul de timpului recuperare, care poate fi înțeleasă ca perioada de timp după un dezastru în care

operațiunea de afaceri este reluată sau resursele sunt din nou disponibile pentru utilizare (ISO, 2018). De exemplu, dacă RTO este de 2 ore, înseamnă că dorim să reluăm livrarea produselor sau a serviciilor sau executarea activităților în maxim 2 ore. RTO este utilizat pentru a determina, în termeni de bani, facilități, telecomunicații, sisteme automate, personal etc, care sunt pregătirile necesare pentru un eventual dezastru. Aceasta implică o dependență firească: cu cât RTO este mai scurt, cu atât sunt mai mari resursele necesare pentru realizarea acestui obiectiv.

Obiectivul timpului de recuperare ar putea fi diferit pentru recuperarea din întreruperi planificate, neplanificate sau dezastre, iar diferite tehnologii de rezilienţă a datelor vor avea durate RTO diferite. Valorile pentru RTO ar putea fi următoarele (IBM, 2019):

- este acceptabil mai mult de 4 zile;
- între 1 şi 4 zile;
- mai puţin de 24 de ore;
- mai puţin de 4 ore;
- mai puţin de 1 oră;
- aproape de zero (aproape imediat).

Este posibil să se obțină un RPO de aproape zero sau chiar zero pierderi de date, dar aceste soluții tehnologice pot fi foarte scumpe. Companiile trebuie să vină cu un obiectiv realist care să le funcționeze.

Obiectivul punctului de recuperare (RPO – Recovery Point Objective) se referă la *volumul de date* pe care compania își poate permite să îl piardă în cazul unui dezastru. S-ar putea să fie necesar ca datele să fie copiate într-un centru de date la distanță, Cloud, etc, astfel încât o întrerupere să nu conducă la pierderi de date. Sau am putea decide că pierderea datelor acumulate într-o perioadă de cinci minute, o oră sau chiar o zi ar fi acceptabilă. Se poate privi și diferențiat pe părți din structura totala a datelor pe care le deține compania și pentru care putem seta obiective în funcție de importanța acestora.

Totuși, conform ISO 22301 (ISO, 2012), definiția obiectivului punctului de recuperare poate fi înțeleasă cel mai bine dacă ne întrebăm, pentru o anumită operație, cât de multă pierdere de date ne putem permite în termeni de timp sau în ceea ce privește cantitatea de informații.

Spre exemplu pentru o bază de date ce conține înregistrarea tuturor tranzacțiilor dintr-o bancă (de exemplu, plăți, transferuri, programare etc.), baza de date care trebuie recuperată trebuie să fie practic egală cu baza de date în momentul dezastrului (adică diferența aproape de zero), deoarece chiar și în doar câteva minute, se pot face sute de tranzacții, iar aceste informații nu pot fi pierdute și nu poate fi recuperate cu ușurință în alt mod. În acest caz, RPO este aproape de zero, ceea ce înseamnă că backup-ul trebuie făcut în timp real.

Pentru un depozit de cod sursă însă, spre exemplu GitHub, este relativ ușor să se rescrie o zi pierdută de scriere a codului pentru un dezvoltator de software, dar mai mult decât atât poate fi dificil sau imposibil de recreat. În acest caz, RPO ar fi de 24 de ore, ceea ce înseamnă că backup-ul trebuie făcut cel puțin la fiecare 24 de ore. Ideea este că, cu cât mai greu se poate de recuperat sau de recreat datele, cu atât mai scurt trebuie să fie obiectivul punctului de recuperare.

Așadar, RPO este utilizat pentru determinarea frecvenței backup-urilor făcute pentru a recupera datele necesare în caz de dezastru. Dacă, spre exemplu, s-a stabilit ca RPO este de 4 ore, atunci trebuie de efectuat backup cel puțin la fiecare 4 ore. Backup-ul făcut la fiecare 24 de ore ar putea să ne pună într-un mare pericol, pe când unul făcut la fiecare oră, s-ar putea să ne coste prea mult și să nu aducă beneficiu afacerii.

RPO al unei entități se află de obicei în unul dintre următoarele intervale (Druva, 2020):

- *Până la 1 oră*. Acest interval este pentru operațiuni critice care nu își permit să piardă mai mult de o oră de date. Aceste operațiuni sunt dinamice, au un volum mare și sunt dificil sau imposibil de recreat din cauza numărului de variabile implicate. Aici se încadrează spre exemplu înregistrările pacienților, tranzacțiile bancare sau sistemele CRM.

- *1 - 4 ore*. Acest interval este pentru unitățile semi-critice ale afacerii, care își pot permite pierderea în valoare de date de până la patru ore, cum ar fi serverele de fișiere și jurnalele de chat ale clienților.
- *4-12 ore*. Unitățile afacerii din acest interval ar putea include date despre vânzări și marketing.
- *13 - 24 de ore*. În acest interval se includ unitățile care gestionează date semi-importante, iar RPO al lor ar trebui să nu depășească 24 de ore. Aici pot fi incluse, de exemplu, achizițiile și resurse umane.

Atât RTO, cât și RPO sunt mărimi ce definesc timpul și, deși par similare, au un scop diferit, așa cum vom prezenta în continuare (figura 1). Pentru ca o companie să-și stabilească obiective de recuperare realiste și realizabile este necesar ca aceste diferențe să fie pe deplin înțelese. Ambele aceste mărimi sunt determinate în timpul analizei impactului asupra afacerii (BIA - Business Impact Analysis), iar pregătirile pentru realizarea acestora trebuie să fie definite în strategia de continuitate a afacerii.

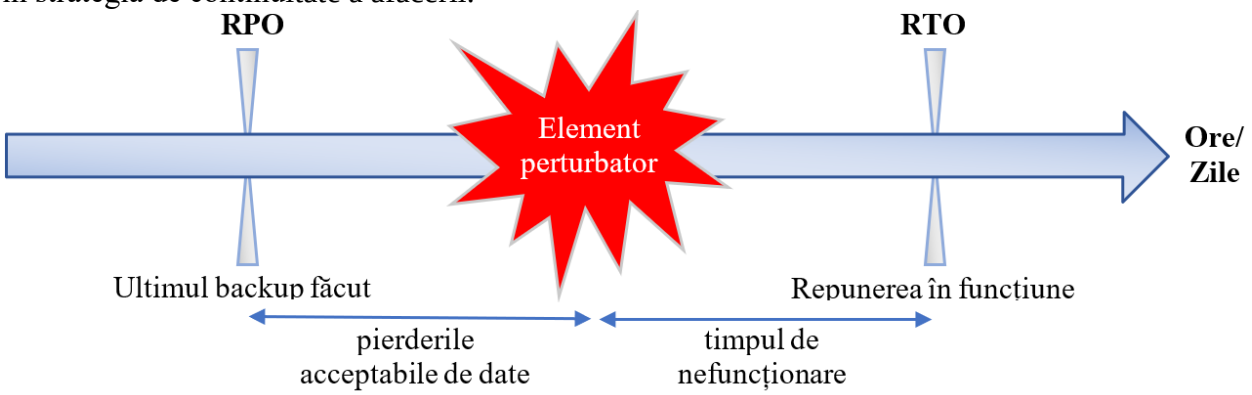

Figura 1. Locul PRO și RTO în procesul de recuperare în caz de dezastru

BIA include necesitatea de a cunoaște o estimare pierderilor dacă compania ar fi offline pentru unele perioade de timp și care ar fi pierderile în caz de pierdere a datelor. Aceste costuri includ atât venituri pierdute, precum și cheltuielile necesare pentru recuperarea după un dezastru. Când o companie începe să elaboreze cerințele sale RPO și RTO, trebuie să ia în considerare nu numai timpul și banii, ci, după cum am menționat încă la început, și reputația. Cât timp și-ar permite compania să fie offline și câte date ar putea ea pierde, înainte de a începe să piardă clienți și reputație?

Unul dintre primii pași pentru o companie atunci când analizează implementarea unui plan de recuperare în caz de dezastru este identificarea aplicațiilor cheie și evaluarea cerințelor RTO și RPO ale acestora. Deși RTO și RPO sunt ambele cruciale atât în analiza impactului asupra afacerii cât și pentru managementul continuității afacerii, ele nu sunt direct relaționate. În același timp ele nu intră în conflict, adică nu este necesar să le contrapunem atunci când planificăm strategia de continuate a afacerii, deci RPO nu este necesar să fie mai mic decât RTO sau invers - am putea avea un RTO de 24 de ore și un RPO de 1 oră, sau un RTO de 2 ore și un RPO de 12 ore.

De exemplu, este posibil ca pentru un site de comerț electronic să fie necesar să fie online peste 4 ore după o întrerupere, deci valoarea RTO este de 4 ore. Acum, același site de comerț electronic poate avea două baze de date, una pentru catalogul său de produse, care se actualizează o dată pe săptămână, iar a doua pentru înregistrarea vânzărilor (mii pe zi). RPO pentru prima bază de date poate fi de 1 săptămână, dar pentru a doua, RPO ar trebui să fie aproape de zero.

4. Relația dintre RPO și RTO

Obiectivul punctului de recuperare indică frecvența copiilor de rezervă care sunt acceptabile pentru întreprindere și determină astfel momentul în care datele pot fi recuperate. În plus, acest indicator caracterizează:

- frecvența operațiunilor pentru copiile de rezervă;
- cantitatea de date noi pe care întreprinderea riscă să le piardă.

RPO este fundamental diferit de obiectivul timpului de recuperare. Cu ajutorul RTO, este posibil de a înțelege cât va dura restaurarea unui sistem sau a unei aplicații sau restaurarea accesului la un set de date după un eveniment neplanificat cauzat de erori umane, defecțiuni ale echipamentului sau dezastre naturale. RTO definește durata perioadelor de nefuncționare (și, prin urmare, costul, riscul și pierderea veniturilor) pe care organizația este dispusă să le tolereze în caz de întrerupere sau dezastru. De multe ori, sunt stabilite diferite obiective de recuperare a datelor pentru diferite tipuri de date și tipuri de defecte - de exemplu, două ore pentru un fișier sau e-mail pierdut, șase ore pentru pornirea unui server avariat și două zile pentru recuperarea după o defecțiune a întregului site sau sistem.

Deoarece RPO și RTO sunt concepte fundamental diferite, mulți sunt interesați de influența reciprocă a acestor doi parametri. De regulă, la această întrebare se răspunde negativ, după cum am afirmat și în compartimentul anterior, dar modul în care obținem RPO se reflectă cel mai direct în respectarea RTO.

Să exemplificăm pentru o bază de date foarte mare, care poate fi copiată doar într-o perioadă suficient de lungă, precum este weekendul. Pentru a reduce RPO de la 48 la 24 de ore, jurnalele bazei de date sau redo-log-urile trebuie făcute în fiecare noapte. Ca urmare, se poate restabili ultima copie completă a bazei de date și apoi executa din nou orice tranzacții care au fost stocate în jurnalele bazei de date sau în redo-log-uri.

Numărul și dimensiunea fișierelor care trebuie recuperate și utilizate împreună cu fișierele bazei de date pot crește foarte repede, mai ales dacă avem de-a face cu un mediu clusterizat la scară largă, cum ar fi Oracle Real Application Clusters (RAC). Aici apare întrebarea rezonabilă: timpul necesar pentru a restabili ultima copie de rezervă completă și toate jurnalele va fi același ca și RTO pentru un sistem mare de baze de date? Răspunsul este în mod evident "nu", cu excepția cazului în care RTO se măsoară în săptămâni și luni. Această metodologie de protecție a bazei de date poate fi utilizată pentru a crea obiective acceptabile pentru punctele de recuperare, dar nu este adecvată pentru îndeplinirea obiectivelor acceptabile pentru timpul de recuperare.

Aici se observă o situație similară cu backup-urile tradiționale complete, la care le mai adăugăm pe cele incrementale. Cu acest model, de obicei se creează o copie de rezervă completă în fiecare weekend și o copie de rezervă incrementală în fiecare zi în timpul săptămânii de lucru. Dacă eroarea sau defectul a avut loc luni și trebuie de efectuat o restaurare completă, acest lucru nu ar trebui să fie dificil: datele sunt restaurate de la ultima copie de rezervă, efectuată în weekend. Dacă eroare s-a produs vineri, trebuie de restaurat copia de rezervă completă din weekendul anterior, apoi, secvențial, toate incrementările care s-au făcut de luni până joi. Procedura de recuperare va dura mult mai mult vineri decât luni. Este oare luat în considerare acest fapt în RTO? De asemenea, recuperarea la sfârșitul săptămânii este un proces mult mai riscant, care implică mai mulți pași manuali. Este posibil ca unele dintre datele recuperate să fie rescrise de până la patru ori.

Evident, pe măsură ce volumele de date continuă să crească și sistemele IT devin mai complexe, abordările utilizate vor trebui îmbunătățite pentru a îndeplini cerințele de backup (RPO) și recuperare (RTO). Compania Hitachi, spre exemplu, oferă o soluție care poate proteja bazele de date mari și aplicațiile de o importanță critică și poate îmbunătăți esențial performanțele RPO și RTO. Această soluție include trei componente (Hitachi, 2020):

- tehnologii de replicare, bazate pe instantanee și stocare, care exclud din sistemul de gestionare a bazelor de date operațiunile de protecție a datelor; elimină necesitatea unei ferestre de rezervă și a timpului de nefuncționare asociat; permite efectuarea copiilor de rezervă mult mai frecvent, reducând cu 90% sau mai mult cantitatea de date noi supuse riscului;
- snapshot-uri și software de replicare pentru aplicații și baze de date care pun bazele de date și aplicațiile într-o stare pregătită (dezactivată) pentru realizarea de backup; creează un instantaneu în mediul de stocare, după care baza de date și aplicația sunt eliberate pentru funcționarea normală; asigură recuperarea rapidă și complet consecventă a operațiunilor în câteva minute, nu săptămâni;
- servicii de evaluare și implementare, care identifică și configurează soluția optimă pentru mediul unic al întreprinderii.

Pentru a vedea dacă PRO nu reprezintă un posibil preț ascuns în RTO, să punctăm ce se conține în RTO. În funcție de definiția specifică, aceasta poate include unele sau chiar toate dintre următoarele aspecte:

- durata studiului și diagnosticului evenimentului;
- durata acțiunilor corective: instalarea unui nou server, înlocuirea unui disc, eliminarea angajatului care a cauzat problema, transferarea operațiunilor la un centru de rezervă;
- durata reinstalării sistemului de operare și a aplicațiilor atunci când apare nevoia;
- durata restaurării tuturor datelor relevante dintr-un sistem de backup sau de recuperare în caz de dezastru;
- timpul necesar pornirii și testării mediului restaurat.

Toate acestea duc la o procedură foarte lungă și implică perioade de nefuncționare. Pentru o anumită perioadă de timp, o parte a întreprinderii este incapabilă să se angajeze în activități productive, care afectează venitul brut sau profitul, sau ambele dintre acestea. În plus, există un parametru care rămâne adesea în afara cadrului listei specificate, dar care se reflectă cel mai direct în durata recuperării complete și în costul total al recuperării. Acesta este obiectivul punctului de recuperare. Dacă RPO este de 24 de ore (de regulă, backupul se efectuează noaptea), atunci acest lucru înseamnă că compania este gata să se împace cu pierderea datelor noi primite în timpul zilei.

RPO este adesea ales din motive practice: de exemplu, un anumit sistem poate fi oprit doar noaptea sau în weekend, cu toate acestea, RPO ar trebui determinat ținând cont și de cerințele comerciale, nu doar de limitările software-ului disponibil pentru copiile de rezervă. Să ne imaginăm că RPO are 24 de ore, iar sistemul se blochează la ora 18 și toate datele conținute acolo sunt șterse sau distruse. Putem, desigur, să le restaurăm de la ultima copie de rezervă, dar toate informațiile create și modificate după aceea vor fi pierdute.

Suntem oare gata să acceptăm pierderea acestor date? Poate că acolo erau mai multe comenzi mari din sistemul de vânzări, rezultatele proiectării pentru ziua respectivă și multe alte informații importante pentru organizație. Toate aceste date trebuie restaurate, adică reintroduse. Acest proces va necesita ceva timp, timp în care angajații ar putea să fie antrenați în activități creative, iar întârzierea, din nou, are un impact negativ asupra eficienței afacerii pe întreaga perioadă de recuperare.

Astfel, cu cât intervalul dintre operațiunile de rezervă (RPO) este mai mare, cu atât vor trebui recuperate mai multe date în cazul unei defecțiuni și cu atât sunt mai mari cheltuielile generale. Mai mult, este posibil să nu existe doar costuri materiale, am putea spre exemplu fi puși în situația să rugăm un client să repete o comandă de un milion de dolari pe care am plasat-o anterior, deoarece sistemul nostru a căzut, ceea ce va lovi destul de dur în reputație.

5. Aspecte ale calculului PRO și RTO

Atât RTO cât și RPO reprezintă calcule (estimări) referitoare la risc. RTO reprezintă o estimare a timpului în care o companie își poate permite o întrerupere a serviciului, iar RPO este o estimare la cât de recente vor fi datele atunci când ele vor fi recuperate după un dezastru.

Calculul RTO se bazează pe prognozarea și gestionarea riscurilor. O aplicație frecvent utilizată poate fi critică pentru continuitatea afacerii, în același mod în care o aplicație utilizată rar. Prin urmare, importanța unei aplicații nu este neapărat direct proporțională cu frecvența de utilizare. Trebuie să decidem pentru fiecare serviciu cât timp acestea pot fi indisponibile fără un impact major și dacă sunt critice sau nu pentru afacere.

Pentru a calcula obiectivul timpului de recuperare este necesar de a lua în considerare următorii factori:

- costul unei ore de întrerupere;
- importanța și prioritatea sistemelor individuale;
- pașii necesari pentru atenuarea sau recuperarea după un dezastru (inclusiv componente sau procese individuale);
- ecuația cost/beneficiu pentru soluțiile de recuperare.

Pentru a analiza adecvat acești factori este necesar de a face o listă cu fiecare sistem și aplicație pe care compania le folosește în mod obișnuit. Aceasta include și identificarea echipelor sau a utilizatorilor finali care ar fi afectați de inaccesibilitatea acestora. Apoi, trebuie de luat în considerare pierderile care ar putea apărea dacă sistemul sau aplicația respectivă ar fi deconectată. Cât de mult s-ar produce venituri și cheltuieli pierdute din cauza lipsei de acces?

Pentru a calcula RTO al unei aplicații ar trebui să răspundem la următoarele întrebări, care ne vor ajuta în acest sens:

- Avem noi grijă de datele pentru clienții noștri? Dacă da, ce acorduri de nivel de serviciu avem cu clienții? Aceasta va indica cât de repede trebuie să putem recupera datele despre clienți.
- Dacă una dintre bazele de date ale companiei s-a deconectat, ce aplicații ar fi afectate și care sunt RTO-urile lor?
- Ce aplicații sau servicii pentru clienți pot duce la nemulțumirea acestora sau chiar la pierderi financiare dacă devin indisponibile pentru clienți? Un exemplu ar fi un site de comerț electronic.

După ce am stabilit timpul de recuperare necesar pentru aplicațiile și bazele de date, RTO general poate fi elaborat în trei moduri:

1. dacă există o aplicație care va provoca o pierdere semnificativ mai mare afacerii decât altele, este recomandat de utilizat timpul necesar pentru a recupera aceasta ca RTO de bază;
2. dacă toate aplicațiile sunt la fel de valoroase, RTO general va reprezenta o medie a timpului pentru toate aceste aplicații;
3. este, de asemenea, posibil să avem cerințe RTO diferite pentru diferite seturi de aplicații.

Odată ce am stabilit RTO pentru o aplicație, sistem sau set de aplicații și sisteme, putem implementa soluția adecvată pentru a satisface acest obiectiv, iar odată stabilite și soluțiile, ele trebuie documentate și testate pentru a ne asigura că cerințele pot fi îndeplinite.

Calculul RPO la fel se bazează pe estimarea riscului. În caz de dezastru, un grad de pierdere a datelor poate fi iminent. RPO devine un act de echilibrare între impactul pierderii de date asupra afacerii și costul atenuării acestuia. Câțiva clienți nemulțumiți din cauza că comenzile lor sunt pierdute, ar putea să fie o pierdere acceptabilă. În schimb, sute de tranzacții pierdute ar putea fi o lovitură de proporții pentru o afacere.

Există mulți factori care influențează RPO general al afacerii, iar acesta va varia în funcție de fiecare aplicație. Mai jos sunt prezentați câțiva dintre acești factori:

- pierderea maximă admisibilă de date pentru organizația specifică;

- factorii specifici industriei - întreprinderile care se ocupă de informații sensibile, cum ar fi tranzacțiile financiare sau dosarele medicale, trebuie să se actualizeze mai des;
- opțiunile de stocare a datelor, cum ar fi fișierele fizice versus stocarea în cloud, pot afecta viteza de recuperare;
- costul pierderii datelor și al operațiunilor pierdute;
- schemele de conformitate includ prevederi pentru recuperarea în caz de dezastru, pierderea datelor și disponibilitatea datelor care pot afecta întreprinderile;
- costul implementării soluțiilor de recuperare în caz de dezastru.

După cum afirmă Nick Cavalancia, consultant cu experiență vastă în domeniu, am putea estima obiectivele de recuperare în caz de dezastru parcurgând patru pași de bază (Cavalancia, 2019):

1. *Analiza operațiunilor afacerii*. Din perspectiva operațiunilor, afacerea are anumite așteptări cu privire la disponibilitatea anumitor date, aplicații și sisteme. În primul rând este necesar de inițiat discuții cu echipa executivă a companiei, proprietarii afacerii, proprietarii de aplicații etc., pentru a afla care sunt nevoile lor în sens de disponibilitate a sistemelor.
2. *Definirea timpului de nefuncționare pentru fiecare set de date*. Pentru fiecare aplicație, set de fișiere, sistem sau combinație a acestora, este necesar de cerut echipei executive să comunice modul în care va fi afectată afacerea dacă fiecare componentă nu este disponibilă. Aceștia trebuie să decidă ce fel de perioade de nefuncționare și pierderi de date pot accepta compania. În final, ar trebui să avem o listă cuprinzătoare a necesităților de recuperare ale întregului mediu al companiei.
3. *Traducerea necesităților în obiective de recuperare în caz de dezastru*. În esență, punctele 1 și 2 ar trebui să ne ofere contextul necesar pentru stabilirea RTO-urilor și RPO-urilor pentru fiecare parte a activității. De exemplu, dacă echipa executivă spune că nu poate fi lipsită de e-mailul local mai mult de o oră și nu poate pierde mai mult de 30 de minute de date, aceasta înseamnă că avem un RTO de 1 oră și un RPO de 30 de minute, în cazul in care nu sunt influențate spre micșorare de alte servicii sau cerințe.
4. *Adaptarea necesităților la posibilități*. În ciuda faptului că echipa executivă poate avea anumite obiective, este posibil ca acestea să nu fie compatibile cu infrastructura actuală de backup și recuperare a companiei. La acest pas este necesar de a analiza cerințele pentru obiective, de a le compara cu ceea ce este posibil și de a stabili obiective realizabile. De asemenea, ar trebui să revenim la echipa executivă pentru a le arăta acest decalaj și a cere un buget mai mare, menționând că nevoile afacerii nu sunt satisfăcute cu infrastructura actuală.

Urmând acești patru pași, am putea răspunde la trei întrebări foarte importante pentru procesul de recuperare în caz de dezastru și implicit pentru continuitatea afacerii:

- Ce necesită afacerea?
- Cum arată obiectivele de recuperare ale afacerii?
- Este posibil să atingem aceste obiective?

6. Concluzii

Nimeni nu poate prezice un dezastru, cu toate acestea, putem acționa organizat urmând planul nostru de continuitate a afacerii atunci când ne confruntăm cu un astfel de incident. Valorile RPO și RTO pot varia în funcție de companii, dar vor fi în orice moment un compromis între nevoile afacerii pentru disponibilitate și investițiile necesare în IT. Estimarea lor ar trebui să fie rezultatul unei deliberări între afacerea organizației și experții IT.

O companie își poate distruge reputația foarte repede în urma unei perioade lungi de nefuncționare cauzată de un dezastru IT. Chiar dacă dezastrele se pot întâmpla oricând oricărei

companii, modul în care o companie gestionează recuperarea în caz de dezastru va avea un impact asupra costului perioadelor de nefuncționare. Timpul inactivității poate fi cuantificat prin cantitatea de pierderi a productivității, a veniturilor și, de asemenea, a reputației.

Pentru ca o afacere să se recupereze rapid după orice dezastru, este important ca ea să-și poată îndeplini obiectivul timpului de recuperare și obiectivul punctului de recuperare ca parte a planului de recuperare în caz de dezastru. Îndeplinirea acestor obiective este imposibilă fără achiziționarea unor aplicații software sau servicii cloud pentru realizarea copiilor pentru backup și recuperare în caz de dezastru. Aceste aplicații și servicii nu vin cu un preț mic, dar reprezintă o investiție bună în comparație cu pierderile provocate de un dezastru. Este decizia companiei după calcularea RTO și RPO de a alege investiția care merită banii.

Menținerea continuității în afaceri mai mult înseamnă pregătire și mai puțin presupunere. Continuitatea afacerii și soluțiile de recuperare în caz de dezastru sunt lucruri pe care organizațiile trebuie să le aibă implementate și care să fie funcționale. O organizație trebuie să găsească echilibrul potrivit între cantitatea de resurse ce vor fi investite în recuperare și un plan de recuperare infailibil elaborat. Pentru a atinge acest echilibru, RPO și RTO sunt esențiale în crearea copiilor de rezervă și recuperarea sistemelor, aplicațiilor și datelor. Fără a determina corect RPO și RTO, procesul s-ar reduce la ghicire și presupunere nefondată, iar acesta nu este cel mai bun mod de a gestiona o afacere.

Referințe bibliografice

1. Cavalancia N. (2019). How to determine your disaster recovery objectives. Available at: https://searchdisasterrecovery.techtarget.com/tip/How-to-determine-your-disaster-recovery-objectives.
2. Druva Documentation (2020). Recovery point objective. Available at: https://www.druva.com/glossary/what-is-a-recovery-point-objective-definition-and-related-faqs/
3. Hitachi Vantara Corp (2020). Data Protection: Downtime Is Money. Smarter Approaches to Data Protection and Recovery. April 2020, 10 p. Available at: https://www.hitachinext.com/en-us/pdfd/white-paper/data-protection-downtime-is-money-whitepaper.pdf)
4. IBM Documentation (2019). Recovery time objective (RTO). https://www.ibm.com/docs/ro/i/7.4?topic=criteria-recovery-time-objective-rto
5. IBM Security (2020). Cost of a Data Breach Report 2020, 82 p. Available at: https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/.
6. ISO 22300:2018. Security and resilience -Vocabulary. 35 p.
7. ISO 22301:2012. Societal security. Business continuity management systems. Requirements. 32 p.
8. SM EN ISO/IEC 27001:2017. Tehnologia informației. Tehnici de securitate. Sisteme de management al securității informației. Cerințe. 42 p.
9. SM ISO/CEI 27031:2013. Information technology. Security techniques. Guidelines for information and communication technology readiness for business continuity, 32 p.
10. Veeam Backup & Replication 11 (2021). User Guide for VMware vSphere. Page updated 4/27/2021. Available at: https://helpcenter.veeam.com/docs/backup/vsphere/backup _window.html?x-clickref=1100lhqsIuIT&ver=110.
11. Zerto Platform (2020). Disaster_Recovery 101, 26 p.
12. ZGUREANU, A. (2020) Strategii de backup și recuperare și rolul lor în continuitatea afacerii. In: Economic security in the context of sustenable development, conf, șt. intern., 11 decembrie, 2020, Chișinău, ASEM, 2021, pp. 285-293, ISBN 978-9975-155-01-4.